SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH POOKIERAMSEY438@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 2:21-mj-00157 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jonathan R. Casto, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer ("TFO") with the Drug Enforcement Administration ("DEA"), and have been since April 5, 2018. I have received DEA TFO training in Norfolk, Virginia. I am currently assigned to the DEA Charleston District Office in Charleston, WV. I have

also been assigned to, or assisted, the Parkersburg Narcotics Task Force ("PNTF") since 2015. I have been a law enforcement officer since 2003.

3. During my 17 years as a law enforcement officer I have been assigned to uniform patrol, in addition to spending time as a detective and a K-9 handler. I am currently assigned to narcotics investigations. While working in uniform, and being a K9 handler, I have had the opportunity to respond to, and investigate, many crimes including narcotics-related crimes. As a detective/agent assigned to the Parkersburg Narcotics Task Force and as a TFO with the DEA, I began to specialize in narcotics related investigations. I have participated in approximately 500 separate narcotics investigations. I have participated in multiple large-scale Drug Trafficking Organization ("DTO") investigations involving multiple jurisdictions and states. I have had the opportunity to assist other federal agencies in cases involving Title III communication interceptions. I have participated in the debriefing of defendants, witnesses, and informants, during which time I have discussed with them their methods of drug smuggling, distribution, packaging, trafficking, and laundering proceeds, among other subjects related to drug trafficking. I have been to a plethora of narcotics-related trainings including, but not limited to, DEA TFO course, DEA concealment methods, dark web training, Ohio Highway Patrol Interdiction Course, K-9 handler courses, and FBI Title III training. Agents and detectives that I work with on a day-to-day basis have had similar, and in some cases more, experience with large-scale narcotics investigations. I have also received instruction and training related to intercepting communications and conducting coordinated surveillance.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the distribution and possession with intent to distribute controlled substances in violation of Title 21, United States Code, section 841(a)(1);

(ii) conspiracy to commit and attempts to commit these offenses, in violation of Title 21, United States Code, Section 846; and (iii) use of communications facility in facilitating the commission of the foregoing offenses, in violation of Title 21, United States Code, Section 843(b) ("the SUBJECT OFFENSES") have been committed by Robert SANDERS Jr., (hereinafter "SANDERS" or "RS"), and others. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

5. Among other duties, I am participating in an investigation relating to the distribution of controlled substances by members of a drug trafficking organization ("DTO") including CARLO LEE RAMSEY; SANDERS; FLOYD DERMONTA RAMSEY; JAMAAL ALEXANDER STOKES, and other persons known, and others as yet unknown (the "SUBJECT INDIVIDUALS" or "SUBJECTS").

6. Beginning on 07/09/2021, the Honorable Irene C. Berger, United States District Court Judge in the Southern District of West Virginia, entered an order authorizing the interception of wire communications over a cellular telephone used by CARLO RAMSEY (SUBJECT TELEPHONE #1). Beginning on 7/30/2021, the Honorable Irene C. Berger, United States District Court Judge in the Southern District of West Virginia, entered an order authorizing the interception of wire communications over a cellular telephone used by SANDERS (SUBJECT TELEPHONE #2), and beginning on 8/12/2021, the Honorable Irene C. Berger, United States District Court Judge in the Southern District of West Virginia, entered an order authorizing the interception of wire communications over a cellular telephone used by FLOYD RAMSEY (SUBJECT TELEPHONE #3). Intercepted communications occurring over the SUBJECT TELEPHONES have confirmed that the SUBJECTS are heavily involved in distributing large quantities of methamphetamine, cocaine, heroin, and marijuana in and around Wood County, West Virginia

and within the Southern District of West Virginia. Intercepted communications over the SUBJECT TELEPHONES have established that SANDERS is a drug trafficker who focuses on methamphetamine and marijuana. From information learned during the investigation, SANDERS is known to utilize iMessage over an iPhone device for communications related to drug trafficking.

7. Surveillance officers have observed SANDERS facilitate drug transactions and collect drug proceeds, as confirmed by communications intercepted over the SUBJECT TELEPHONES.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Summaries of recorded conversations set forth in this affidavit are based on draft transcripts of those conversations. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

10. SANDERS, also known as "Pookie," is a courier/distributor in the DTO.[1] In November 2018, SANDERS was arrested for possession with intent to deliver methamphetamine

[1] Agents are aware from experience dealing with SANDERS that he commonly uses the nickname "Pookie."

and marijuana in connection with a previous Parkersburg Narcotics Task Force ("PNTF") investigation. SANDERS was observed by agents of the PNTF getting off a commercial bus line and then entering a vehicle operated by EMORY BYRD. A traffic stop was then conducted by agents, resulting in SANDERS being arrested due to his possession of approximately two pounds of methamphetamine and approximately one pound of marijuana. SANDERS was later convicted of the felony offense of possession with intent to deliver a controlled substance on or about April 19, 2019, in Wood County (West Virginia) Circuit Court due to this incident. SANDERS is currently on parole from this arrest/conviction. SANDERS also has a previous conviction for felony possession of drugs from the Washington County (Ohio) Court of Common Pleas with a conviction date on or about July 26, 2012. Beginning on 07/09/2021, investigators have intercepted numerous telephone calls involving SANDERS relating to the acquisition and distribution of controlled substances and proceeds from the distribution of controlled substances.

11. On 07/31/2021 Patrol Officers with the Parkersburg Police Department Uniformed Division conducted a traffic stop and subsequent arrest of Matthew DEPEW (hereinafter "DEPEW"). During DEPEW's arrest he was found to be in possession of approximately 112 grams of suspected methamphetamine. During processing of DEPEW he agreed to speak with patrol officers in reference to where he obtained the methamphetamine. During a mirandized statement DEPEW told officers he obtains a significant amount of methamphetamine from a male known to him as "Ramsey". DEPEW also stated that the methamphetamine in his possession came from "Ramsey." Officers obtained the telephone number of (304) 494-1599 (the number then associated with SUBJECT TELEPHONE #2) for "Ramsey". When Officers told me the phone number I knew the number to belong to SANDERS from this investigation. I later obtained a search warrant from a Wood County Circuit Judge for an Apple iPhone that was in the possession of DEPEW at the

time of his arrest and obtained a cell phone extraction report. In the report I found that SANDERS was communicating with DEPEW through iMessages involving controlled substances. I later found that DEPEW's phone number did not appear in toll records for SANDERS telephone number. I learned that iMessages do not utilize cellular telephone towers and are not sent through a phone provider, and that iMessages are sent through data just like using an application. Accordingly, iMessages are not available through a cell phone provider. On 08/04/2021 a preservation request was sent to Apple Inc. for the iCloud account with account name "POOKIERAMSEY438@iCloud.com." I learned that SANDERS utilizes this iCloud account name from four receipts obtained from Enterprise Rent-A-Car bearing dates between January and April 2021, with the most recent receipt bearing the date of 04/15/21. "Pookie" is a nickname commonly used by SANDERS. Although his last name is Sanders rather than Ramsey, SANDERS is related to several members of the Ramsey family including Carlo RAMSEY and Floyd RAMSEY, and his mother's last name is known to investigators to be Ramsey.

12. In the cell phone extraction report from DEPEW's phone, it is shown that on 07/09/2021, SANDERS used SUBJECT TELEPHONE #2 to send and receive a series of iMessages with DEPEW. SANDERS said "I am here", "my fault wrong person", "and ok the so you good then". DEPEW responded "lol I was like huh but I could grab three rn but anything on the arm be cool lol" "yo that was a 7 not 3". SANDERS then responded "ok" "send me your address". From my training and experience and knowledge of this investigation, and the interview with DEPEW, I know this conversation to be about DEPEW obtaining controlled substances from SANDERS. When SANDERS asks DEPEW "and ok so you good then" I know SANDERS to be asking DEPEW if he still had an amount of controlled substances. When DEPEW responds "lol I was like huh but I could grab three rn but anything on the arm be cool lol" I know this to mean he

wants to obtain three possible ounces of controlled substances from SANDERS and when DEPEW says "on the arm" he means to be fronted or to obtain the controlled substances first and pay SANDERS later. On 07/18/2021, DEPEW and SANDERS again exchanged iMessages. DEPEW sent an iMessage to SANDERS on SUBJECT TELEPHONE #2 stating "U round?." SANDERS responded "yeah it's gone be later tho". DEPEW responded "like late late?" SANDERS responded "Probably so". DEPEW then said "Damn well HMU need 12". SANDERS affirmed by saying "ok then". From my training and experience, and knowledge of this investigation, I know that when DEPEW is asking SANDERS for "12" he is attempting to obtain an amount of controlled substances. When SANDERS responds "ok then" I know this to mean SANDERS is agreeing to provide DEPEW with the requested amount of controlled substances. Based on the investigation so far, I know that the user of SUBJECT TELEPHONE #2 is SANDERS, and that DEPEW was contacting SANDERS on SUBJECT TELEPHONE #2 in furtherance of drug trafficking.

13. On 08/02/2021, at approximately 4:16 P.M. (session 120), SANDERS, using SUBJECT TELEPHONE #2, placed an outgoing call to KAITLYN SIMMONS ("KS" below), believed to be the girlfriend of MATHEW DEPEW, at (304) 494-3857. The following was discussed:

KS: Hello.

RS: Hey, yo! Uh, what's up with uh, Matt ma'am. They just told me the news.

KS: Uhm, yeah, he got pulled over yesterday. Not yesterday, I think it was Saturday the 31st, he got pulled over and... they caught him with some shit and then they, then they searched my house.

RS: Damn!

KS: Found some guns so... He wanted to, he wanted to say that, he has his part, that he has his shit hauled down to, like change your number and shit.

RS: Yeah, I'm definitely about to do that and shit, yeah. Yeah, I'm definitely want to do that.

KS: Yeah. They said, he said, he told me to say that he, his phone has a lock on it but just in case.

RS: Yeah. He end up [U/I].

KS: 'Cause they definitely got it.

RS: Yeah, I'm definitely gonna do that. Damn!

KS: Yeah.

RS: When uh, when his court day is?

KS: Uhm, I'm not sure but usually they have it within 10 days.

RS: Okay then.

KS: But I'm if you... you have Facebook?

RS: Nah, ain't got, no ain't got none of that.

KS: I was gonna say, I'd let, I'll let you know. I'll just let you know what happens but.

RS: Alright then.

KS: But I'm forgetting your number changed then, I won't a have way to get.

RS: No, I mean, I mean, no I'm gonna keep this number for a couple of more days then [U/I] change it.

KS: Alright.

RS: Definitely, yeah definitely keep me posted.

KS: Alright, I will.

RS: A'ight.

Based on my training, experience, and the facts of the investigation, I know this conversation is SANDERS asking KAITLYN SIMMONS about the circumstances of DEPEW's arrest. ("Uh, what's up with uh, Matt ma'am. They just told me the news.") KAITLYN SIMMONS then explains the circumstances of what occurred to SANDERS and advises SANDERS to change his phone number. ("change your number and shit"). SANDERS responds by saying that he will change his number, likely due to concern about investigators obtaining a search warrant for DEPEW's phone and discovering the drug trafficking discussions between SANDERS and DEPEW that are housed on DEPEW's phone. ("Yeah, I'm definitely about to do that and shit, yeah. Yeah, I'm definitely want to do that.") KAITLYN SIMMONS confirms that investigators did get DEPEW's phone ("'Cause they definitely got it"), but stated that the device is locked. ("They said, he said, he told me to say that he, his phone has a lock on it but just in case.") SANDERS then affirms that he will change his number in a couple days. ("No, I mean, I mean, no I'm gonna keep this number for a couple of more days then [U/I] change it.") To date, SANDERS is still utilizing SUBJECT TELEPHONE #2 although he did obtain a new phone number from Verizon on or about 08/12/2021.

14. On several occasions, despite the wire communications of SANDERS being intercepted over SUBJECT TELEPHONE #2 since 07/23/2021 and SUBJECT TELEPHONE #1 since 07/09/2021, and his electronic communications being intercepted over SUBJECT TELEPHONE #2 since 8/12/2021, SANDERS has been observed by investigators travelling to cities such as Seattle, Washington, Baltimore, Maryland, and Thomasville, North Carolina, for suspected controlled substance transactions without any accompanying wire or electronic communications to provide context for these trips. For that reason, in conjunction with SANDERS' use of iMessages to communicate with DEPEW, investigators believe that SANDERS

is using iMessages to arrange and coordinate meetings with some of his suppliers, customers, and co-conspirators. Therefore, access to these iMessages as well as the account information needed to confirm SANDERS' association with the above-cited iCloud account name is likely to allow investigators to obtain valuable evidence regarding SANDERS and his role in committing the SUBJECT OFFENSES on behalf of the DTO.

BACKGROUND CONCERNING APPLE[2]

1. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

2. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and iCloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

---

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via iCloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

3. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @iCloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

4. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

5. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

6. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition,

information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through iCloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

7. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

8. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. I know from the facts of this investigation that SANDERS utilizes an iPhone and uses iMessages to have conversations with other subjects due a cell phone extraction of an iPhone utilized by DEPEW after his arrest. I know that iMessages are not sent through a cell phone provider but are sent over the internet utilizing data.

9. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. I know from the facts of this investigation that SANDERS utilizes iMessages to communicate due to a cell phone extraction of an iPhone utilized by DEPEW after his arrest.

10. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access

the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

11. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

12. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. I know from the facts of this investigation that SANDERS, as well as other SUBJECT INDIVIDUALS, utilize cash app to send money back and forth. I also believe that SANDERS, as well as other SUBJECT INDIVIDUALS, have accounts for "whats app" which is an encrypted communications application.

13. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users. I would ask that Apple be ordered to disclose any and all requested information that was generated between July 9, 2021 and August 23, 2021.

CONCLUSION

14. Based on the forgoing, I request that the Court issue the proposed search warrant.

15. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

16. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Jonathan R. Casto, Task Force Officer for the
Drug Enforcement Administration

Subscribed and sworn to before me on August 24, 2021

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with "POOKIERAMSEY438@iCloud" that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 4, 2021, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. The contents of all instant messages associated with the account from July 9, 2021, to August 23, 2021, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

c. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

d. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

e. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

f. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **10 days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 21 U.S.C. § § 841 or 846, those violations involving **ROBERT SANDERS, JR.,** and occurring after July 9, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Drug trafficking and any activities undertaken to further or assist drug trafficking, including but not limited to arranging meetings with suppliers, customers, co-conspirators, and others associated or involved with drug trafficking;

(b) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(c) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(d) The identity of the person(s) who communicated with the user ID regarding drug trafficking and any activities undertaken to further or assist drug trafficking, including records that help reveal their whereabouts.